Cloud Bleeding-Typos Leaking Your Information

Nupur Baisakhiya
Department of Technology Management, School of Engineering
University of Bridgeport, Bridgeport, CT

What is Cloud Bleeding : Cloudflare, which is used by more than 5.5 million websites, accidentally leaked mass amounts of sensitive user information from those sites, including passwords, private messages, hotel bookings, and more between September 2016 and February 18th of this year.
The leak has been dubbed '<u>Cloud Bleed</u>'.

What is Cloud Flare : Cloudflare is a popular content delivery network and according to their site, "provides performance and security", including DDoS protection for millions of websites, including Medium, Feedly, FitBit, TransferWise, Zendesk, OK Cupid and more.

Who are affected ? How?

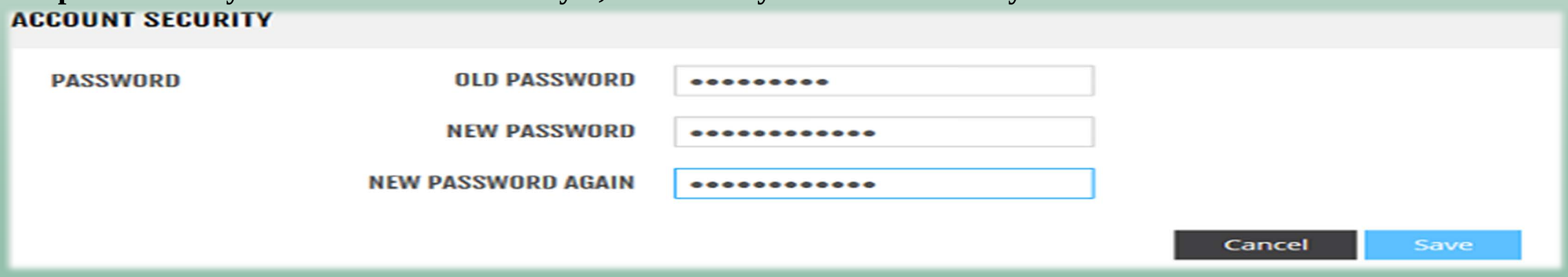
It's our data which is affected by <u>Cloud Bleed</u>. Cloudflare has not formally released a list of affected websites. However , unofficial list of 4,287,625 possibly-affected domains that use Cloudflare DNS, not just the Cloudflare proxy that was primarily affected. Some of the major, notable sites include:
Uber.com,Fitbit.com,Yelp.com,Okcupid.com,Change.org,Zendesk.com,Medium.com,Patreon.com,Jquery.com,Glassdoor.com

A bug in Cloud flare's code has led an unknown quantity of data—including passwords, personal information, messages, and more—to leak all over the Internet. *Is this the first you're hearing about <u>Cloud Bleed</u> vulnerability? Buckle up. This is kind of scary.*
The root cause of the bug was that reaching the end of a buffer was checked using the equality operator and a pointer was able to step past the end of the buffer. This is known as a buffer overrun. Had the check been done using >= instead of == jumping over the buffer end would have been caught. Hence , user valuable data could have been saved. Cloud bleed involves a buffer overflow vulnerability that results in web session and leaks and private data exposure.

```
/*Generated Code*/
If (++p == pe)
    goto_test_eof;
```

Are you in trouble? What should you do? How to Protect Yourself From Cloud Bleed?

- ✓ **Rotate your website passwords—all of them. Because Cloud flare's CDN services are in use by the internet's most prominent brands, users of all major websites should change their passwords immediately.**
- ✓ **Users should also log out and log in to their mobile applications to save your confidential information.**
- ✓ **Users are strongly encourage to use strong, unique passwords on each and every one of your accounts to prevent a hacker from access multiple accounts if one is compromised.**
- ✓ **Use security questions to protect your bank accounts with very strong password.**
- ✓ **Make use of Multifactor authentication on every Website possible.**
- ✓ **Recommended resetting two-factor authentication tokens for accounts where it's enabled, since 2FA codes may have been compromised. If you haven't enabled 2FA yet, make sure you do so for all of your accounts whenever it's available.**



Conclusion and Some Lessons from this Typo Bug Leakage

- ✓ **Its very important for users to be aware of any doubtful activity in their accounts and must make very strong password. Updating your passwords may seem like a mountain of a task, but the costs of not doing so leave much more at stake**
- ✓ **The engineers working on the new HTML parser had been so worried about bugs affecting our service that they had spent hours verifying that it did not contain security problems. Unfortunately, it was the ancient piece of software that contained a latent security problem and that problem only showed up as we were in the process of migrating away from it.**
- ✓ **Cloud bleed illustrates the inherent fragility of today's digital supply chains and how flaws in third party code can introduce vulnerabilities into the most secure systems, potentially damaging the world's most trusted digital brands.**

References:
Bleeding clouds: Cloudflare server errors blamed for leaked customer data . (2017, Feb 23). *CSO FROM IDG*. Retrieved from http://www.csoonline.com/article/3173639/security/bleeding-clouds-cloudflare-server-errors-blamed-for-leaked-customer-data.html
Incident report on memory leak caused by Cloudflare parser bug . (2017, Feb 23). *Cloud Flare*. Retrieved from